COVID-19 Pandemic and Post-pandemic: Impact and Technical Threats in India

Aastha Tyagi and Madhu Sharma Gaur

Abstract World Health Organization declared Coronavirus as a pandemic. More than 6 million confirmed cases of COVID-19 have been found leading to more than 367166 deaths till May 31, 2020. With every passing day, the number of cases and deaths is expanding. The widespread of this epidemic has not only threatened human health but also production, economy, social functioning, education, etc. In this critical pandemic situation, a large number of the population are fighting for their lives and economic challenges for survival. Although digital health would not be the main contributor in combating COVID-19, it could play a very important supporting role in control and prevention work. During this isolation period, various digital applications are needed to ensure a normal life for most of the people. Artificial intelligence, machine learning, data analytics, big data, cloud computing, Internet of things (IoT) and other digital technologies are playing a vital role in managing routine activities through work from home, online education, remote patient treatment, citizen protection, risk communication, and medical supplies. On the downside, various technical threats like online fraud and cyber-attacks are rising and increasing challenges in the COVID-19 pandemic. The objective of this paper is to explore the available COVID-19 statistics and understand the impacts with technical threats to relief measures in India caused in the current pandemic. To realize social responsibility and comprehend response capacity in foreseeing COVID-19 extortions and foster the community awareness toward population and public health allocation where upholding local health with technical risk prevention is alarming. In the winding up, post-pandemic open challenges are also discussed.

Keywords Corona virus · COVID-19 · Cyber threats · Cyber security · Cyberspace · Impacts · Pandemic opportunities · Post-pandemic challenges

A. Tyagi (✉) · M. S. Gaur
G.L. Bajaj Institute of Technology and Management, Greater Noida, GautamBudh Nagar, UP, India
e-mail: aasthatyagi90561@gmail.com

M. S. Gaur
e-mail: madhu14nov@gmail.com

R. Agrawal et al. (eds.), *Advances in Smart Communication and Imaging Systems*,
Lecture Notes in Electrical Engineering 721,
https://doi.org/10.1007/978-981-15-9938-5_46

1 Introduction

In the month of December 2019, in China Wuhan City, a mysterious pneumonia killed many people and also infected more than seventy thousand individuals. As per World Health Organization (WHO), the virus that causes this disease "Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-Cov-2)", disease was named as novel Coronavirus or COVID-19. It belongs to the family of Coronaviridae. The disease COVID-19 was named by the combination of two words (Corona + Virus) where Corona means a part of body resembled to be a crown-like spike found on the outer surface of the virus. The virus is contagious and rapidly spreading through human-to-human transmission. Initially, it was reported in the people who had travel history being transmitting. As the year 2020 starts, the virus spread worldwide and COVID-19 was announced and from the January 2020 to till now virus infection transmission continues and has huge impact on the worldwide society. On March 11, 2020, World Health Organization (WHO) classified this virus as pandemic [1]. Around 8098 individuals were infected around the world by SRAS-CoV (2003) [2], on the other hand, COVID-19 infected 6 M individuals leading to 367 K deaths around the world, till date of this writing.

2 Related Work

Some researchers have been made considering threats and relief measures from COVID-19 so far. Different authors have suggested different measures to control and prevent people. In [1], Mouton and Coning, talk about various areas which create a larger impact from cyber security perspective on COVID-19 like misinformation, fear mongering (panic buying), fake URLs and malicious Web site. It talks about only two measures, i.e., node VPN and cyber measure. According to International Criminal Police Organization (INTERPOL) [3], in order to take advantages of online behavior and trends (COVID-19 outbreak), cyber threats are constantly evolving. It talks about the three types of cyber-attacks in COVID-19 like malicious domain, malware, ransomware. It also provides some recommendation and tips to prevent from these threats as by keeping information safe, securing email gateways, performing regular scans on computer and mobile devices.

Analysis of malware that supersedes the system master boot record was done by Trend Micro in [4], analyzed (April 24) about a malware based on coronavirus theme, making it unbootable. It also mentioned about some other type of threats using COVID-19 such as spam, mobile ransomware (CovidLock) an android application that helps to track COVID-19 cases but actually locks the phone of victims. A cloud app security by Trend Micro provides solution to defense against these threats in which it finds unknown malware using machine learning. As per the recent Technical Analysis report by VMware [5], COVID-19 has generated a "substantial

uptick" in cyber security attacks, leading to "high-level risk for both personal security as well as corporate security". According to this report, phishing emails are the primary source of attack where unauthorized users use techniques like fake links in emails and attachments to deliver malicious software to recipients. In [6], Matt J Keeling discussed the ability to produce intended result through contact tracing. It mentioned about the main advantage of contact tracing as it is an effective and robust technology, which can identify the person before severe symptoms emerge and can prevent onward transmission.

3 COVID-19 Epidemic

Since December 2019, Coronavirus has spread rapidly nationwide in China and now by the month of January 2020 it reached worldwide. Everyday number of positive cases are being confirmed and deaths being reported of less immune and aged people. As per available sources, in India, on January 30, 2020, first Corona positive case was reported in Kerala in a student who came for vacation from China. The student was studying in Wuhan University, China, returned to India and was found Corona positive. Although in the month of February 2020, the virus transmission was very slow, as by the end of February only three Corona positive cases were confirmed. Figure 1 shows confirmed cases in India from January 30, 2020–February 29, 2020.

But due to certain events like Tablighi Jamaat event, panic buying, escaping of suspected people, misinformation and discrimination, there is a sudden increase in the number of individuals affected by it. In March, these cases rise from few to 1 K as shown in Fig. 2.

By April 29, 2020, the Ministry of Health and Family Welfare has confirmed 31,332 cases, leading to 1007 deaths and 7797 recoveries (1 migration), in India [2] which increased as shown in Fig. 3.

On May 18, 2020, some zones were being unlocked. On May 19, 2020, the cases reached to 100 K. As on May 31, 2020, there were 182,143 active cases being reported as shown in Fig. 4. In the coming month, there will be the hype in these cases.

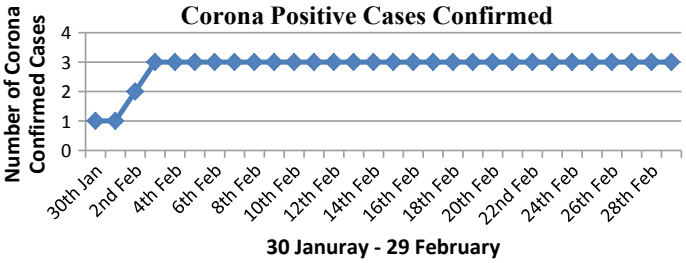

Fig. 1 Corona positive cases confirmed in India, January 30–February 29, 2020 [7]

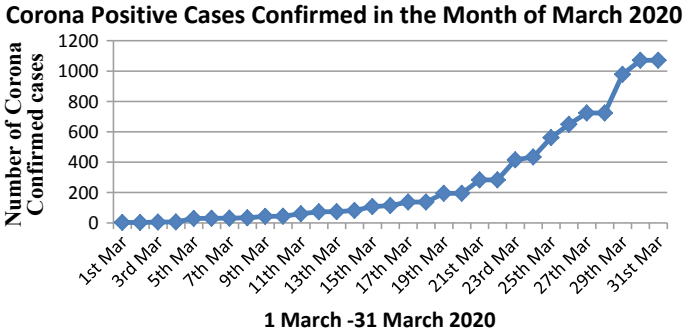

Fig. 2 Sudden increase of confirmed cases in India (March report) [7]

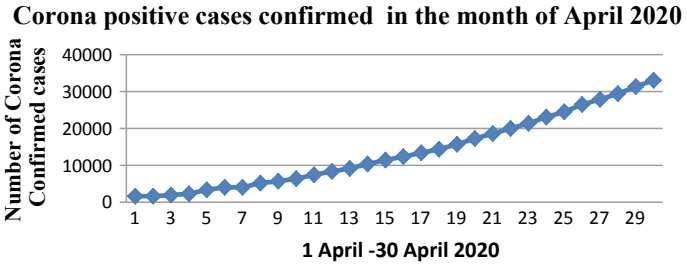

Fig. 3 Worse situation due to the increased number of cases (April report) [7]

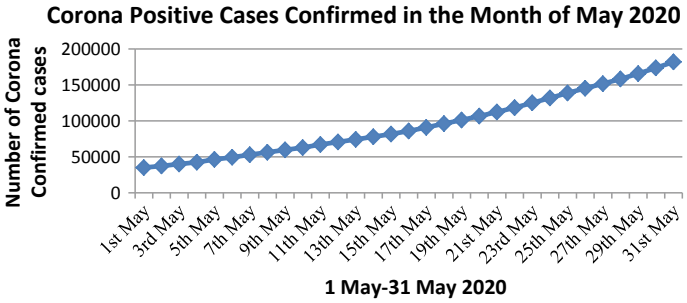

Fig. 4 Cases in India have crossed 1,00,000 (May report) [7]

Since January 31 (when the first case was identified in India) till May 31, the cases are being increased leading to 5164 deaths. Figure 5 shows the confirmed cases from January–February to May 2020 with the linear increase.

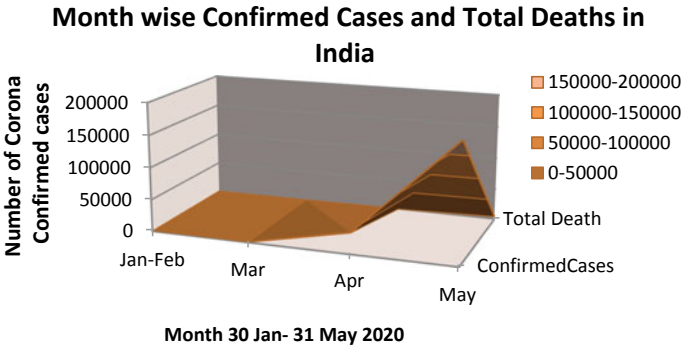

Fig. 5 Month wise (January–May 2020) confirmed cases and total death in India by the end of month

4 COVID-19 Rise and Outbreak in India

4.1 Top Seven Indian States Where Rising Corona Cases

In India, the cases of COVID-19 are going to reach 200 K leading to more than 5 K deaths [7]. Table 1 shows seven states of India where the cases are increasing gradually.

When the first case was detected in India, since then lots of actions are being taken by Indian government to control the increase in the cases. To maintain social distancing, lockdown has been imposed in the whole country. Various applications are being launched to fight against COVID-19. Following is the chronological list of COVID-19 rise and what India has gone through the period when first case was detected on January 30, 2020 to March 31, 2020.

Table 1 List of top seven states of India where Corona cases increased rapidly [8]

S. No.	Indian state	Number of Corona confirmed cases (in Thousands—K)
1	Maharashtra	70 K
2	Tami Nadu	23 K
3	Delhi	20 K
4	Gujarat	17 K
5	Rajasthan	8980
6	Madhya Pradesh	8283
7	Uttar Pradesh	8075

Table 2 Chronological list of rising COVID-19 outbreak in India

Year	Date	Event
2019	?	Mysterious phenomenon in Wuhan, Hubei, China
	December	First confirmed case in Wuhan
2020	January 30	First case in India (Kerala)
	March 5	Sudden increase in the number of confirmed cases (29 confirmed case) in India
	March 25	21 days lockdown(25 March 2020–14 April 2020)
	March 30	More than 1000+ confirmed cases identified in India
	April 2	Launching of AarogyaSetu (application to fight against COVID-19) app in India
	April 14	The confirmed increases from 1 to 10 k leading to 339 deaths Lockdown 2.0 till May 3, 2020
	April 28	First update of AarogyaSetu
	April 30	33,050 (confirmed cases), 1074 (deaths) in India
	May 18	Lockdown 4.0
	May 19	101,139 (confirmed cases), 3163(deaths)in India
	May 30	Lockdown 5.0 in containment zone till June 30, 2020 173,763 (confirmed cases), 4971 (deaths) in India

4.2 Events in COVID-19 Outbreak

See Table 2.

5 Threats Caused Due to COVID-19 and Relief Measure Taken

5.1 Technical Threats

Due to the shift of remote work (work from home), organizations are more vulnerable to rising cyber-attacks. In the mid of the month of March, rapidly number of Corona cases being rising and by the Govt. complete lockdown was declared in India on March 24. On the same time, many Indian companies noticed a massive number of attacks too. There are many types of technical threats using COVID-19 [1, 4, 6, 9].

Cyber Threats during COVID-19 lockdown: During lockdown work from home, online business, online study increasing cyber threats and other technical challenges.

As India was facing spike in COVID-19 cases, there is also an increase of COVID-19 information emails. Some emails are related to charity, researches or some claims to provide essentials to the one in need. Due to this situation, there is a threat of becoming

cybercrime target is rising by opening those emails. Many offices have provided their own laptop to their workers which are on the target of being attacked and hence leading to attacking the online meeting being organized. [10]. Some common attacks are as follows:

Phishing: It is one of the easiest forms of cyber-attack for an attacker to carry out; through it, they can invade every important thing of their target's lives. Most of the time, phishing has been witnessed in the wild in emails. More than 900 k threats are there across email, URL and file according to data collected by smart protection network. Certain phishing Web sites were being remarked and are now blocked:

- adaminpomes[.]com/em/COVID-19/index-2[.]php
- bookdocument[.]in/Covid-19/COVID-19/index[.]php
- glofinance[.].com/continue-saved-app/COVID-19/index[.]php
- laciewinking[.]com/Vivek/COVID-19/

Malicious Web Site: It is a Web site created when a scammer links a user to a Web site that looks exactly like a familiar site but is actually the scammer's site. Increase impact of COVID-19 results in the threat caused by two Web sites; "antivirus-covid19[.]php" and "corona-antivirus[.]com" which is now inaccessible. According to Trend Micro, there were more domains that were also found malicious as given below:

- Accorona[.]com
- beatingcoronavirus[.]com
- bestcorona[.]com
- coronadatabase[.]com
- corona-crisis[.]com and many more.

Fake Maps: This was developed to silently steal passwords, crypto wallets and other sensitive information. The cyber-attackers made a "fake" version of the map provided by Johns Hopkins University named as deadly Coronavirus map.

Mobile Threats: CovidLock(mobile ransomware) tracks COVID-19 cases. Actually, this malicious android application locks the phone of victims and demand for some ransom from the victim to gain access to their phone. Otherwise, they might delete the victim's important data or might leak social media account details. As per VMware Carbon Black, the fake android Coronavirus app was discovered as follows:

- COVI (com.droobihealth.corona)
- Corona Virus Status (com.arumcomm.coronavirusstatus)
- Coronavirus (coronavirus.tracker.news)
- COVID-19 Alert (corona.report).

Sextortion Scam: Sextortion is an attempt to extort money or get victims do something against their will by threatening the victim to release their personal images and videos. The images may be fake imagery such as sextortion scams. According to certain sources, in this scam the victim gets email with respect to danger that

Table 3 List of data breaches, ransomware, malicious insiders and miscellaneous incidents (March 2020)

Entity	Records	Method	Ref
Tesco	600,000	Credential stuffing attack	[11]
Boots Advantage Card	150,000	Hacking	[12]
Hammersmith Medicines Research (attack on COVID-19, former patients record)	Unknown	Maze ransomware attack	[13]
Vijay Sales (India)	Unknown	Data breaching	[14]
Henry Mayo Newhall hospital	1	Snooping medical record	[15]

scammer knows every one of their mysteries, their passwords, their whereabouts and different subtleties identified with individual exercise (Table 3).

5.2 COVID-19 Frauds in India

EMI moratorium fraud: Reserve Bank of India (RBI) first declared the moratorium on loan EMI for next 3 months (from March 1 to May 31, 2020) and now it has been further extended to 3 month (June 1 to August 31, 2020) [16]. It means in this duration, the borrowers will not have to pay EMIs and other loan. Due to this, cybercriminals get the chance to trick people. In EMI moratorium fraud, attacker calls the borrower as their bank representative and asks for OTPs or passwords to gain access to the bank detail of the customer by offering them extend their EMI payment. The borrower loses money when they share their details with the fraudsters.

Fraud in PM CARES FUND: In the Prime Minister's Citizen Assistance and Relief in Emergency Situation Fund, the national fund is raised for endangering situation like COVID-19 pandemic. Main objective of this PM CARES FUND is to provide relief and render financial assistance to enhance the critical healthcare facilities, etc. [17]. Basically in PM CARES Fund fraud, fake Unified Payment Interfaces (UPIs) are being used. The correct UPI ID is "pmcares@sbi". Generally, the fake UPI IDs are omitting the letter "s" from PM CARES. The fake UPIs mentioned by CERT-in (Indian Computer Emergency Response Team) are pmcare@sbi, pmcares@pnb, pmcare@yesbank and pmcare@icici [18].

Fake E-commerce Web site: During this pandemic, the customer usually prefers to purchase product online by keeping them safe, and it is also easy to use. Therefore, cybercriminals take a huge advantage of it by developing fake e-commerce Web site selling essentials. The site is similar to the original site in which you can select item, provide your address details and make payment. After that the site is shut and your item never gets delivered [19].

Malware installation: According to some resources, many domains with name containing Corona, COVID, virus and many more were being registered for phishing attacks. The most well-known video conferencing application during nowadays is Zoom, and there is an abrupt increment in the new area enlistment with names including Zoom. These domains contain malware, once the user clicks on it, which leads to malware attack on their device [20].

5.3 Technical Relief Measures

Contact Tracing: It is the process of identification of undiscovered individual who may have come into contact with a tainted individual. This helps to reduce infection in the population. The purposes of contact tracing are as follows:

- To reduce spread of the infection by interrupting this transmission.
- To aware, alert and prevent people from contacting to the possibility of infection.
- To offer diagnosis to those who are infected.

Certain mobile applications are designed for preventing 2019–20 Coronavirus pandemic to aid contact tracing like:

- *AarogyaSetu* (launched by Government of India): This app uses GPS location and Bluetooth to track users. It also guides for self-isolation and is also aware about COVID-19 symptoms and precautions [21].
- *BeAware Bahrain* (developed by iGA (The information of eGovernment authority)): This app went through BETA testing, and it is compulsory for all the quarantine cases to register in it, whereas other can register by their valid IDs or passport number [22].
- *CoronaApp* (developed by the Colombian Government): It helps to detect nearby areas and individuals infected by COVID-19. It also contain technologies developed by Government of Singapore, Government of South Korea and Apple [23].
- *eRouška application* (launched in Czech Republic): It is based on Bluetooth technology. If the permission is granted by user, then the phone with active Bluetooth will help to know about both infected and non-infected person as they meet [24].

India takes action against the prevention of COVID-19 by launching many mobile applications. These applications are as in Table 4.

Table 4 Action against the prevention of COVID-19

Application name	Launched by developed by	Different features
AarogyaSetu	Government of India	• This app tells about the low, moderate or high risk when a non-infected person meets an infected person • Works on Bluetooth proximity • Available in 11 languages
COVA Punjab	Government of Punjab (India)	• Works on real-time dashboard for Punjab stats • Traveler and shop registration feature(updated on April 29)
CG COVID-19 ePass	Government of Chhattisgarh	• Issue state wise and intra-district wise e-pass for vehicular movement to transport essential commodities • e-pass generated by photograph, valid ID proof and business proof
Test Yourself	Government of Goa/Innovanccer Inc.	• Self-evaluation assessment for risk identification
Quarantine Watch	Revenue Department, Government Of Karnataka	• Self-reporting by home quarantine persons

Certain features to be added in an application for combating against COVID-19

1. Travel history of the person should also be recorded if he travels from hotspot area to green area. (Hotspot areas are those areas where more than six people have been tested positive of Coronavirus)
2. Alert message while entering in the red zone, i.e., hotspot zone.
3. Map of area with zone highlighted (low, moderate, high risk zone) nearby the individual location.
4. COVID-19 prevention-related games for children which should be aware of them and also productively passes theirquarantine time.
5. Some healthy tasks and videos should be available on the app so that individual can utilize their time.
6. Aware every individual about cyber-attacks which is also creating a huge impact on lives.

Things to keep in mind:

- Not to reveal your information to strangers whether they claim they are from your bank, company or any government organization.
- Do not open attachments from unknown sources.
- Avoid using unauthorized applications or software.
- Check the details correctly while transferring money digitally.

- There are many known and well-established Web sites, therefore buy items from them only otherwise prefer buying items locally.
- Better to verify the identity of the receiver before helping them.

5.4 Impact of COVID-19

On Information Technology: These days major problem faced by the IT industry is because of the economic fall, due to the public health concern companies tell their employees to work from home (remotely). Therefore, there is a huge loss. For example: Due to the unpredictability caused by the outspread of Coronavirus, Apple's stock rises and falls widely. In the mid of February, Apple stock hits a high closing price and by the end of February it dropped. Furthermore, in March, it has also fallen [25]. The Indian IT sector depends upon international clients like Europe and USA, where there is a worse impact of this pandemic. Due to which there may be a worse impact on the Indian IT sector leading to huge losses [26].

On Education: As everything has moved online from education to teaching, this creates an immense revelation on student's social life and learning also [27]. Due to network failure and many uncertainties, many assessments and exams are being canceled or postponed. This is not only an issue for school-going children but it is also affecting many universities as there is a slowdown in student placements and internships.

Internet of Things (IoT): The interest of IoT gadgets has been diminished as clients are staying at home, increased unemployment and lack of income, there is a decrease in the acquisition of IoT gadgets. In India in complete lockdown, due to the decline in budgets of technology, many ongoing projects are being paused. Not only the ongoing projects are being paused as well as the new projects are also declined. Many companies freeze their hiring in IoT firms [28, 29].

Drones: The doctors, the policemen, the security guards, the sanitary workers all are playing a major role in combating COVID-19 similarly technologies like artificial intelligence, big data, GIS and location technology are also playing a vital role in combating COVID-19. The drones also play a key role in helping people and authorities through:

- Surveillance
- Broadcast
- Disinfectant spraying
- Monitoring traffic and lockdown violators.

In many parts of India, drones are being used like in New Delhi, and it is used to enforce social distancing on roads, to keep watch on places where there is a crowd like grocery shops, banks and religious places. In some part of India, it is being

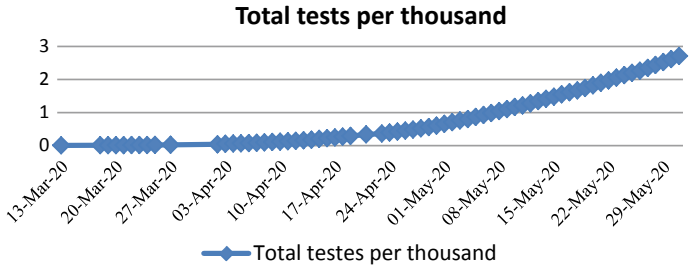

Fig. 6 Total tests per thousand have done in India by May 31, 2020

used for creating awareness among people about the restrictions implemented by administration [30].

Machine learning: Major problem in this pandemic is the lack of testing done. Testing is important to know how many people are infected with this virus. In many countries including India, the limit with regard to COVID-19 testing is still low. Figure 6 shows the total tests done per thousand in India. Machine learning is a significant tool in fighting the current pandemic. In this time, if we take the opportunity to gather information, pool our insight and combine our abilities, we can then save much information—both now and later on.

Through machine learning, we can categorize the population based on gender, age, symptoms and their travel history which can be used further for processing and combating COVID-19 [31].

Blooming opportunities: To fight with this virus, we require three things to cooperate which is primarily focused on better understanding of pandemic challenges and public health risks prevention for population awareness and to get learning from this pandemic and give a social call for preparedness for such future outbreaks. Technology enabled services to contribute in promoting public advisory and guidelines. Here are some opportunities for people during this pandemic:

- Although the information technology is suffering a lot with this outbreak, there are some opportunities opened in IT industry like 5G technology, ecommerce, epayments, Telehealth, etc.
- Students should explore digital learning platforms on their own.
- Lot of internship programs and research projects are available online.
- Support communities should be made for teachers and students for queries.

5.5 Post-pandemic Challenges

The future is never an exact replica of the past, and the universe will see further tragedies, but they are not going to grow just as COVID-19 did. It is necessary to

think beyond this current virus to develop a system that can provide an effective solution to the wider range of future threats, and post-pandemic sustainability imposed many open challenges like reinventing remote health monitoring, telemedicine and teleconsultation, public health and elderly care.

Technological shift and assessing the emerging technical risks with new strategies will be another major challenge for technology leaders working in different domains. Recognizing new world of work with upgrading skills and learning will be the basic course of action remote access, virtual laboratories, virtual business with virtual collaborative space secure accessibility, online education and community events with security and privacy will be a big concern, whether it is a cyber-attack, climate change-fueled disasters or some other possibilities.

Furthermore, the world's battle with the coronavirus is highlighting how risk will spread and intensify one another. Scenarios for the post COVID-19 can be defined as the economic powers may lead to panic and conflicts, exacerbate economic harm (economic reconstruction had to deal with massive debts, broken global trading and investment system), increase in cyber-attacks/cyber threats (cyber-attackers will use this pandemic situation and may cause more harm in future), technology shift in the domain (as everything is moving online people who are facing problem in business, education, online shopping) and decimate the hope of growing out of this crisis.

6 Conclusion

COVID-19 pandemic is increasing day by day. There are many steps taken by the Govt., administrative and healthcare warriors but we can delay the increasing number in India rather than fully control the social, economic and general life-threatening problems. There are social and technical threats have been explored and presented in this paper. A social call is still open to protect our lives from this virus, and on the other side many opportunistic withering minds who are involved in creating technical threats. By being aware of the cybercrimes and growing threats in this pandemic as well as post pandemic can contribute in the race of fighting against COVID-19 with new normal opportunities. Self-care awareness, healthcare best practices and strictly following advisories with better realization of technological threats and opportunities are the best tools to overcome from this pandemic crisis. In every sector, a proper planning and leadership qualities are to be taken to prevent various attacks. As the government is taking action to prevent the people of their countries from pandemic impacts and consequences. Being a socially sensitive community contributor it is also every one's responsibility to keep them safe and beware to challenges and opportunities with countersign impact of open and connected technological inferences to countersign impact and open and connected technological inferences.

References

1. Mouton F, de Coning A (2020) COVID-19 impact on the cyber-security threat landscape, March 2020
2. Adnan Shereen A, Khan S, Kazmi A, Bashir N, Siddique R (2020) COVID-19 infection:Origin, transmission, and characteristics of human coronaviruses, March 2020
3. INTERPOL: International Criminal Police Organization. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.
4. Trend Micro Inc. [US], Developing story: Covid-19 used in malicious campaigns. © 2019 Trend Micro. Updated on 24 April 2020
5. VMWare Carbon Black, Technical analysis: hackers leveraging COVID-19 pandemic to launch phishing attacks, fake apps/maps, Trojans, Backdoors, Cryptominers, Botnets & Ransomware. ©2020 Carbon Black
6. Keeling MJ, Deirdre Hollingswort T, Read JM (2020) The efficacy of contact tracing for the containment of the 2019 Novel Coronavirus (COVID-19). Februrary 2020
7. WHO Coronavirus disease (COVID-19) situation reports. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports
8. Home|Ministry of Health and Family Welfare|GOI. https://www.mohfw.gov.in/. Accessed on 29 April 2020
9. CRN Team, PwC India's Threat Analysis_COVID-19|Significant rise in cyber incidents as hackers exploit the Covid-19 crisis
10. Saran J, Cyber threat in times of COVID-19 outbreak. 8 April 2020. https://www.financialexpress.com/opinion/cyber-threat-in-times-of-coronavirus-outbreak/1921878/
11. Kleinman Z, Tesco sends security warning to 60,000,000 Clubcard holders. https://www.bbc.com.news/technology-51710687
12. Wharton J (2020) Boots Advantage Card hit by cyber attack, 5 March 2020
13. Goodwin B, Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. 22 March 2020
14. India's Vijay, Sales leaks private information through exposed Amazon backup server. 20 March 2020
15. HIPPA Journal, Henry Mayo Newhall hospital fires employees for Snooping on medical records, 13 March 2020
16. ET Online, RBI extends EMI-moratorium for another 3-month on term loans. Here's what it means for borrowers. 23 May 2020
17. PMINDIA, About PM CARES Fund. https://www.pmindia.gov.in/en/about-pm-cares-fund/. Accessed on 25 May 2020
18. CERT-In, Alert people about fake UPI IDs seeking donations towards PM-CARES Fund." Updated on 3 April 2020
19. India's ecommerce growth propelled due to COVID might come at the cost of more online frauds. Published on 18 May 2020
20. COVID-19 Impact: cyber criminals Target Zoom domains. Accessed on 25 May 2020. https://blog.checkpoint.com/2020/03/30covid-19-impact-cyber-criminals-target-zoom-domains/
21. MyGov [IN], Government of India. https://www.mygov.in/aaroogya-setu-app/
22. MGZN Startup, BeAwareBahrain'app officially launched by iGA (31 March 2020)
23. CoronaApp, https://coronaviruscolombia.gov.co/test/aislamiento-saludable/coronapp.html
24. Holzman O (2020) V Česku se spouštíaplikaceeRouška. Stavínaochraněsoukromíaupozorní, pokudjstepřišli do kontaktu s nakaženým (in Czech), 11 April 2020. (The eRouška application is launched in the Czech Republic. It builds on privacy and alerts you if you come in contact with an infected person (English translation))
25. Clover J (2020) COVID-19 Coronavirus impact on Apple's iPhoneMax and WWDC. 14 May 2020. https://www.macrumors.com/guide/covid-19-coronvirus/
26. Raja Simhan TE, Indian IT sector may take a heavy hit as Covid batters US and Europe. Updated on 8 April 2020. https://www.thehindubusinessline.com/info-tech/indian-it-sector-may-take-a-heavy-hit-as-covid-batters-us-and-europe/article32289747.ece

27. Burgees S, Sievertsen HH, Schools, skills, and learning: the impact of COVID-19 on education. 1 April 2020
28. LasseLueth K, The impact of COVID-19 on the (IoT) Internet of Things-now and beyond the Great Lockdown: Part-I. 16 April 2020
29. LasseLueth K, The impact of COVID-19 on the (IoT) Internet of things-now and beyond the Great Lockdown: Part 2. 22 April 2020
30. Chandola S, Drones emerged as go to technology partners to combat COVID-19 India. 13 April 2020
31. Burhanuddin Bhopalwala, COVID-19 and machine learning. 26 March 2020